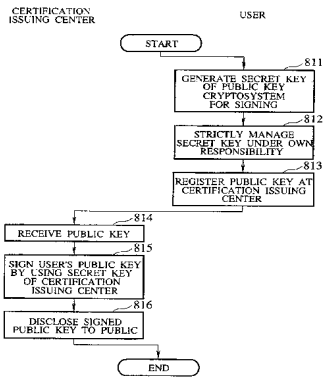
software signature certificate in the manner recited in claim 1 and then why England does not disclose or suggest checking the software signature certificate and signed software for integrity as also recited in claim 1.[1]

The Office Action cites column 5, lines 43-67 of Ishii for the disclosure of the following claim element:

> generating a software signature certificate using the public key of the software signature site and a secret key of a control entity of a trust center, according to a public-key method,

The cited section of Ishii is part of the Summary of the Invention section, which corresponds to the sixth embodiment discussed in connection with FIGs. 22 and 23 of the Detailed Description section. As illustrated in FIG. 22 of Ishii (reproduced on the right), a user's public key is signed using a secret key of the certification issuing center (step 815) and the "signed public key is disclosed to the public as this user's certification (step 816)."[2]

FIG.22



In contrast to Applicant's claim 1 that requires "using the public key of the ***software signature site***", Ishii discloses "a ***user's*** public key". Thus, even if it were assumed that the result of the signing in step 815 of Ishii was a software signature certificate, it would be generated using "a ***user's*** public key" and not "the public key of the ***software signature site***" as required by Applicants' claim 1.

---

[1] This should not be interpreted as an attempt to address the references individually. Instead, Applicants' are directly addressing how each of the cited patent documents is being applied to the claims. Regardless, each claim element that is addressed with respect to a particular cited document is not disclosed or suggested by any of the cited documents, either alone or in combination.

[2] Column 31, lines 12-13.

The discussion in the Response to Arguments section of the Office Action highlights the fact that the rejection is not considering the actual claim language:

> Ishii discloses the generation of a signature (a standard cryptographic processing function) using a public key of one entity and a secret key of another entity. (Ishii col 5, lines 43-67; signing (signature certificate) by using the secret key of certification issuing center (first public key cryptosystem); ...[3]

Applicant's claim 1 does not simply recite generating a signature using public and private keys of two generic entities, but instead specifies that the public key is of a ***software signature site*** and the secret key is of a ***control entity of a trust center***. Thus, a generic disclosure of "using a public key of one entity" does not render obvious the claim requirement of "using the public key of the ***software signature site***". Because Ishii's disclosure of a ***user's*** public key is not the same as the claim requirement of "using the public key of the ***software signature site***"[4], Ishii does not disclose or suggest generating a software signature certificate in the same manner as required by the language of claim 1. England and Wong do not remedy these deficiencies of Ishii.

[3] Page 5.
[4] Emphasis added.

Turning now to the application of England to claim 1, the Office Action cites England as disclosing:

> checking the software signature certificate for integrity according to a public-key method using a public key of the trust center; and

To reject this element set forth above the Office Action states:

> see England col. 8, lines 7-14; certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 8, line 66 – col.9, line 3: trusted third party (use digital signature for authentication); trusted third party equivalent to trust center)[5]

Column 8, lines 7-14 of England discusses a certificate that is created for a CPU. Accordingly, the CPU certificate of England is not the same as the claimed "software signature certificate". As illustrated in column 8, line 66-column 9, lines 3 (reproduced below), England is generically discussing signing software but does not disclose or suggest that a software signature certificate is signed or that such a certificate is signed using a public key, much less a public key of a trust center.

> The first requirement is met in the exemplary embodiment of the invention by having ***all trusted operating system-level components digitally signed*** by their developers or a trusted third-party, with the signature acting as a guarantee that the components respect digital rights.[6]

As such, this generic disclosure of signing operating system-level components does not disclose or suggest the specific requirement of claim 1 that a software signature certificate is signed using a public key of a trust center.

---

[5] Page 8.
[6] Emphasis added.

The Office Action does not explain how England's disclosure of signing trusted operating system-level components relates to the claim recitation of "checking the software signature certificate". Accordingly, Applicants' previous attempted to address this citation to England by explaining that England does not disclose or suggest that a software signature certificate is an operating system-level component. Contrary to the discussion in the Response to Arguments section of the Office Action[7], Applicants were not arguing that the claimed software signature certificate is an operating system component. Quite the opposite, Applicants' were arguing that England's disclosure of signing operating system-level components has no disclosed relationship to the claimed software signature certificate.

Additionally, the discussion in the Response to Arguments section of the Office Action addressing the checking of the software signature certificate again demonstrates that the rejection is not based on the claim language itself, but instead on the idea that generic disclosures of keys and certificates renders obvious the particular keys and certificates recited in claim 1:

> England also discloses utilizing certificates with public and private key pairs with certificates to verify a digital signature.
>
> In addition, England does disclose checking a signature certificate for integrity.
>
> For additional clarity, England discloses a certificate is signed, therefore the certificate can be checked for validity by checking its digital signature. (see England, col. 8, lines 7-14; certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 11, lines 54-59:

[7] Page 2.

> checks signature of a component before loading it; if signature valid then component has not been compromised)[8]

The first two sentences merely state what is asserted to be disclosed by England without any citation of support. As such, these first two sentences do not provide any evidence to support the rejection. The remainder of this discussion confuses England's disclosure of a signed CPU certificate with the verification of operating system-level components. Again, England does not disclose or suggest that a ***CPU certificate*** is a ***software signature certificate***. Additionally, England's disclosure in column 11, lines 54-59 of checking the signature of operating level-system components does not have any relation to checking the CPU certificate discussed in column 8, lines 7-14.

Because there is no evidence in the record that England's CPU certificate is a software signature certificate and the rejection has not cited any other certificate in England, the rejection has provided no evidence that England discloses or suggests "checking the software signature certificate" in the manner recited in claim 1.

The Office Action also relies upon England to reject the following claim element:

> checking the signed software for integrity, using a public key of the software signature site contained in the software signature certificate, the public key of the software signature site being complementary to the secret key of the software signature site.

[8] Page 3.

To reject this claim element the Office Action states:

> (see England col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; col. 11, lines 54-59: checks digital signature of a component before lading it; signature valid then component has not been compromised and loaded)
>
> The digital rights OS components are loaded and the digital signature is checked for each component before loading. And, England discloses a signed digital certificate from the manufacturer of the control unit (CPU) and OS software.
>
> This is equivalent to disclosure in the specification on page 6, paragraph [0021], lines 3-6, that discloses a software signature certificate is generated and signed by the manufacturer of the software.[9]

Column 11, lines 47-59 of England discuses that the signature of software components are checked before they are allowed to be loaded. It does not specify how this check is performed. Indeed, it does not disclose or suggest that this is performed "a public key of the software signature site contained in the software signature certificate" as recited in claim 1.

The citation to the ***CPU certificate*** has no apparent relevance to the claim recitation of checking the signed software for integrity using a public key ***contained in the software signature certificate*** because the CPU certificate is for the CPU and not for software. Additionally, the disclosure on page 6 of Applicants' specification does not indicate an equivalence between a CPU certificate and a software signature certificate.

[9] Page 8.

Although column 11, lines 50-53 of England discloses that all components are signed and "provided with a rights manager certificate", there is no disclosure or suggestion that this certificate includes a public key of a software signature site that is used for checking the integrity of signed software. The rights manger certificate is disclosed in FIG. 9 of England (reproduced below).

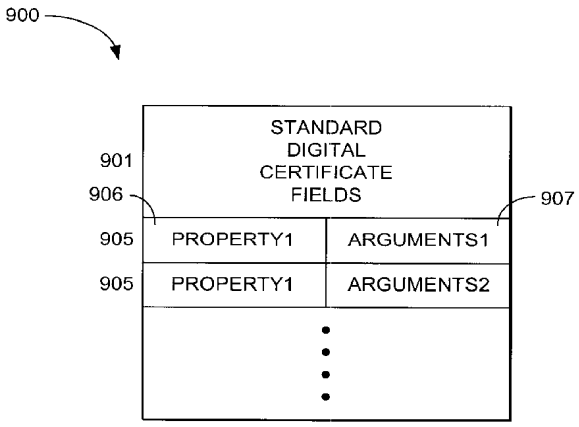


Fig. 9

England describes the certificate as including information related to digital rights management but is silent with respect to the certificate including a public key of a software signature site as recited in Applicants' claim 1:

> A list of application properties 903 is appended to the digital certificate fields 901 standard in some digital certificate format such as X.509. The certificate names the application. Each entry 905 in the list 903 defines a property 906 of the application, along with optional arguments 907. For example, one property might be that the application cannot be used to copy content. Another example of a property is one that specifies that the application can be used to copy content, but only in analog form at 480P resolution. Yet another example of a property is one that specifies that the application can be used to copy content, but only if explicitly allowed by an accompanying license. Additional examples include the right to store an encrypted copy of the content and to restrict such

> storage to only certain, acceptable peripheral devices. The property 906 can also be used to specify acceptable helper applications, such as third-party multimedia processing stacks or other libraries, to be used in conjunction with the application named in the certificate.

Accordingly, there is no disclosure or suggestion in England that the digital rights management certificate includes a public key of a software signature site that is used to check the integrity of signed software as recited in claim 1.

The Response to Arguments section of the Office Action does not provide any evidence that England discloses checking the integrity of the signed software in the particular manner recited in claim 1, but instead that England discloses generically checking the integrity of signed software. Specifically, the Office Action states:

> England discloses that the signature of the boot block is checked before loading the digital rights OS. The software is checked for integrity before its usage as a digital rights OS. (see England col 9, lines 7-10: digital rights OS; col 8, 48-51:system incorporates public/private key pairs, digital certificates; col. 8, lines 34-37: boot block signed by OS manufacturer; (boot block processed before execution or use of software); col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate)
>
> In addition, England does disclose checking a signature certificate for integrity.
>
> For additional clarity, England discloses a certificate is signed, therefore the certificate can be checked for validity by checking its digital signature. (see England, col. 8, lines 7-14; certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 11, lines 54-59: checks signature of a component before loading it; if

> signature valid then component has not been compromised)[10]

The first paragraph reproduced above does not address how England discloses that the software is checked for integrity using a public key contained in a software signature certificate. The second paragraph is not provided with any supporting citation to England, and thus provides no evidence that England discloses that the software is checked for integrity using a public key contained in a software signature certificate. As discussed above, the third paragraph confuses England's disclosure of a signed CPU certificate with the verification of operating system-level components. It does not provide any evidence that the software is checked for integrity using a public key contained in a software signature certificate.

Ishii and Wong similarly do not disclose or suggest checking the software signature certificate and the signed software in the manner recited in claim 1.

Because England, Ishii and Wong each do not disclose or suggest generating a software signature certificate and checking the integrity of the certificate and of the signed software in the manner recited in claim 1, even if one skilled in the art were motivated to combine England, Ishii and Wong, the combination would not disclose or suggest all of the elements of this claim. As such, claim 1 is patentably distinguishable over the combination of England, Ishii and Wong. Claims 3-6, 9, 12-18 are patentably distinguishable at least by virtue of their dependency.

[10] Pages 2 and 3.

As previously discussed, the combination of England, Ishii and Wong does not render claim 7 obvious because the combination does not disclose or suggest a control unit storing:

1. a clearing code site signature certificate,
2. a software signature certificate,
3. clearing code data and their signature; and
4. software and its signature.

Specifically, the cited section of England[11] only mentions that a CPU can be equipped with a pair of public and private keys, but does not mention any certificates, clearing code data or clearing code data signature.

The Response to Arguments section responds to Applicants' argument by stating:

> England discloses a certificate (software signature, clearing code signature) which contains a public/private key pair for each particular certificate. England also discloses (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to the CPU; certificate contains public key)
>
> England discloses the clearing code data (identity) and signature capability for a certification (clearing code certificate. (see England col. 8, lines 26-28; col. 9, lines 4-10; software identity; identify of an authenticated OS)[12]

It appears that the first sentence is attempting to equate certificates with signatures. England, however, clearly distinguishes between certificates and signatures. For example, England discusses signing certificates. If certificates

[11] Column 7, lines 50-54.
[12] Pages 3 and 4.

were the same as signatures, then England would disclose applying a certificate to a certificate, which England does not.

The second paragraph appears to rely upon England's CPU certificate. It does not, however, describe which of the claimed certificates correspond to the CPU certificate. Regardless, England's CPU certificate does not correspond to any of the claimed certificates.

The third paragraph appears to assert that England discloses the claimed clearing code site signature certificate, however, the citations relates storage of the identity of an authenticated digital rights operating system in a CPU. There is no explanation of how storage of an operating system identity in a CPU relates to a clearing code signature site certificate as recited in claim 7.

Ishii and Wong do not remedy the above-identified deficiencies of England, and accordingly the combination cannot render claim 7 obvious.

Regarding claim 19, the combination of England, Ishii and Wong does not render this claim obvious because the combination does not disclose or suggest a control unit that checks whether a ***software signature certificate*** and signed software has been changed or manipulated.

As previously discussed, the Office Action's reliance on England's disclosure of checking software component signatures for validity does not disclose or suggest checking ***a software signature certificate*** for manipulation as required by claim 19.

The Response to Arguments section, however, does not address how England discloses checking the particular certificate recited in claim 19, i.e., the

software signature certificate. Instead, it highlights the Office Action's continued insistence on relying upon generic disclosures to reject the specifics of Applicants' claims. Specifically, the Office Action states that:

> A certificate (***no matter what type***) is still digital information and its integrity can be checked using digital signature verification procedures. England discloses the verification of ***whether digital information (a digital certificate***) has been modified or changed. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised) The Examiner is operating under the assumption that when a component is signed then the component is protected. Any modification or updates to the certificate can be discovered by checking the digital signature.[13]

Simply because England discloses checking the signature of software components, and software components and digital certificates are both digital data does not mean that England discloses or suggests checking the particular certificate recited in Applicants' claim 19, i.e., a ***software signature certificate***. Again, it appears that the rejection ignores the actual claim language in order to support the rejection. This is clearly improper. Ishii and Wong do not remedy this deficiency of England, and accordingly the combination cannot render claim 19 obvious.

Claim 20 is patentably distinguishable at least by virtue of its dependency from claim 19.

For at least those reasons stated above it is respectfully requested that the rejection of claims 1 and 3-20 be withdrawn.

[13] Page 4 and 5. (Emphasis added).

If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323, Docket No. 080437.53236US.

Respectfully submitted,

December 6, 2010

/Stephen W. Palan, Reg. No. 43,420/
Stephen W. Palan
Registration No. 43,420

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP